

REMARKS

This application has been carefully reviewed in light of the Office Action mailed April 23, 2004. Claims 1-17 and 19-21 are pending and stand rejected and Claim 18 is canceled. Applicants have amended Claims 1, 3, 7, 11, 13, 14, 16, 20, and 21. Favorable action is requested.

Rejections Under 35 U.S.C. § 102

The Office Action rejects Claims 1-5, 7-17, and 20-21 under 35 U.S.C. § 102(d) as being anticipated by U.S. Patent No. 5,319,776 issued to Hile, et al ("*Hile*"). Applicant respectfully traverses these rejections for the reasons provided below.

Claim 1 is allowable because *Hile* does not teach or suggest ". . . for each one of the at least one variable character [that is within a REGEX signature]: selecting the variable character as the current character; **generating a state for the current character [which is the variable character]** that is independent of the current character," as recited by Claim 1. The Office Action identifies column 4, line 59 - column 5, line 21 of *Hile* as showing an examination of virus signatures, but neither this identified portion nor any other portion of *Hile* discloses a way to match a REGEX signature having variable characters,¹ and for at least this reason the missing limitation is not shown by *Hile*. Instead of the missing limitation, *Hile* discloses identifying virus signatures having non-variable characters by matching each character of a signature to toggle forward to a new state. If a character is not matched, then a search for a match for the unmatched character continues until a match is finally found so that a next state can be determined for the character. For example, the identified portion of *Hile* discloses identifying virus signatures "tale", "tool", and "ale", which do not include variable characters and thus cannot show the missing limitation. Further, during the matching process, if a character in a virus signature is not found, *Hile* teaches consulting a "failure" table and either (1) revert back to the beginning state of a search by assuming a state of "0," or (2) jump to another state, and from that state, continue to look for a match for the unmatched character. If a match is found, then a state is assigned

¹ In one embodiment, an example of a REGEX signature is provided in the present application as "DOG*.HOME", which indicates that an attack is indicated if: (1) the characters "D", "O", "G" are observed in order; (2) any number of characters occur after the "G"; and then (3) the characters "H", "O", "M", and "E" occur in order. (See page 12, lines 1 through 5 of the present Application.)

to the **matched** character, and the process continues (see column 5, lines 8-16 of *Hile*). Thus, at least according to *Hile*, it appears that a match is required for a state to be assigned to a character. However, *Hile* does not disclose generating a state for the variable character **regardless of what the variable character is**, and thus the missing limitation is not shown. This is advantageous because in some embodiments, an intrusion detection system may not need to examine each character of a signature more than once, at least for purposes of intrusion detection. Thus, fewer processing resources are required for intrusion detection, and a buffer may no longer be needed for the purpose of sufficiently examining a character string for intrusion detection. *Hile* does not benefit from this advantage, as shown in FIGURE 1 of *Hile* by buffers 30 and 38 used for storing a virus signature. ("The input data stream passes from the removable diskette medium into an input buffer 30, whereupon the buffered data is tested for virus signatures" Column 4, lines 45-47). *Hile* does not disclose generating a state for a variable character regardless of what the variable character is, and thus Claim 1 is allowable. Favorable action is requested.

For reasons analogous to those provided in conjunction with Claim 1, Claims 7, 13, 14, 16, and 20 are allowable. Favorable action is requested.

As depending from their respecting allowable independent Claims, depending Claims 2-6, 8-12, 15-17, 19, and 21 are also allowable. Favorable action is requested.

Rejections Under 35 U.S.C. § 103

The Office Action rejects Claims 6 and 19 under 35 U.S.C. § 103(a) as being unpatentable over *Hile* in view of U.S. Patent No. 6,078,924 issued to Ainsbury et al ("*Ainsbury*"). Applicant considers the rejection of Claims 6 and 19 moot in view of the arguments provided above in conjunction with Claims 1 and 16 because Claims 6 and 19 depend from Claims 1 and 16, respectively. Favorable action is requested.

CONCLUSION

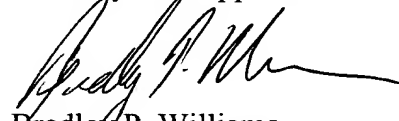
Applicant has now made an earnest attempt to place this case in condition for immediate allowance. For the foregoing reasons and for other apparent reasons, Applicant respectfully requests allowance of all pending claims.

If the Examiner feels that prosecution of the present Application may be advanced in any way by a telephone conference, the Examiner is invited to contact the undersigned attorney at 214-953-6447.

Applicant does not believe that any fees are due. The Commissioner is hereby authorized to charge these fees and any extra fee or credit any overpayments to Deposit Account No. 02-0384 of Baker Botts L.L.P.

Respectfully submitted,

BAKER BOTTS L.L.P.
Attorneys for Applicant



Bradley P. Williams
Reg. No. 40,227

Date: July 21, 2004

Correspondence Address:

Customer Number: **05073**